US009165294B2

US 9,165,294 B2

(12) **United States Patent**
Sharma et al.

(10) **Patent No.:** US 9,165,294 B2
(45) **Date of Patent:** Oct. 20, 2015

(54) **METHOD FOR USING BARCODES AND MOBILE DEVICES TO CONDUCT PAYMENT TRANSACTIONS**

(75) Inventors: **Pankaj Sharma**, Singapore (SG);
Vikram Modi, Laguna Green (SG);
Shantnu Singh, Singapore (SG)

(73) Assignee: **Visa International Service Association**,
San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 181 days.

(21) Appl. No.: **13/594,433**

(22) Filed: **Aug. 24, 2012**

(65) **Prior Publication Data**

US 2013/0048714 A1   Feb. 28, 2013

Related U.S. Application Data

(60) Provisional application No. 61/526,969, filed on Aug. 24, 2011.

(51) **Int. Cl.**
G06K 19/00 (2006.01)
G06Q 20/32 (2012.01)

(52) **U.S. Cl.**
CPC *G06Q 20/3276* (2013.01)

(58) **Field of Classification Search**
USPC 235/487, 492
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,237,164	A	8/1993	Takada
6,202,933	B1	3/2001	Poore et al.
7,225,156	B2	5/2007	Fisher

7,387,250	B2	6/2008	Muni
7,477,780	B2	1/2009	Boncyk et al.
7,634,295	B2	12/2009	Hayaashi et al.
7,680,702	B1	3/2010	Oakes, III
7,810,720	B2	10/2010	Lovett
7,878,400	B2	2/2011	Harris
2002/0069165	A1	6/2002	O'Neil

(Continued)

FOREIGN PATENT DOCUMENTS

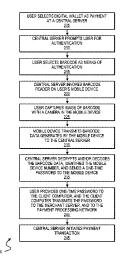|		
KR	1020110026338 A	3/2011
WO	03/023674 A1	3/2003
WO	2010097711 A2	9/2010

OTHER PUBLICATIONS

Zhao, J., et al., "Yet Another Simple Internet Electronic Payment System," Proc. of the IFIP 1996 World Conference—Mobile Communications, Canberra, Australia, Sep. 1996, pp. 1-8.

Primary Examiner — Michael G Lee
Assistant Examiner — Tabitha Chedekel
(74) *Attorney, Agent, or Firm* — Kilpatrick Townsend & Stockton LLP

(57) **ABSTRACT**

Embodiments of the invention facilitate payment transactions by integrating the image capture and image processing capabilities of certain mobile devices with the card-based payment transaction infrastructure. In some embodiments, a camera contained in a mobile device is used to capture an image of a barcode that is visible on the surface of a substrate. The barcode may represent or otherwise encode one or more of payment account data, consumer authentication data, consumer profile data, or other relevant information. In some embodiments, the captured image may be processed by the mobile device to extract the payment account data, authentication data, or other relevant data. This data may then be communicated to a data processing element that is connected to, or forms part of, a payment processing network in order to conduct the desired payment transaction.
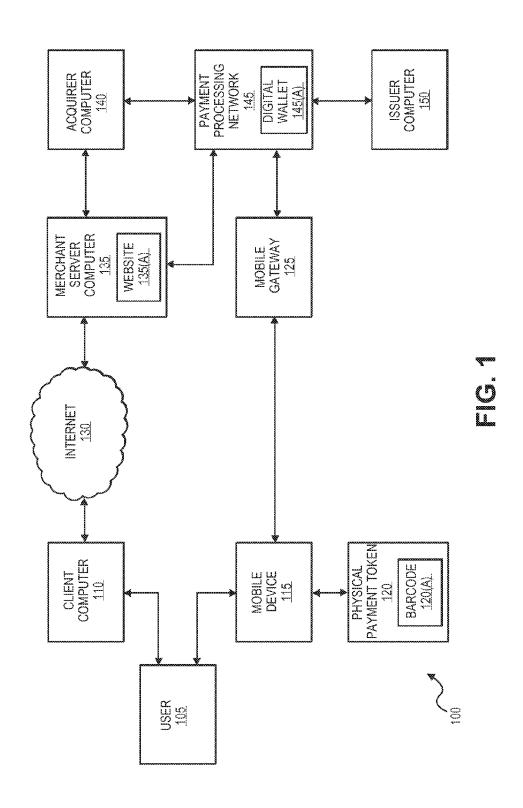
24 Claims, 12 Drawing Sheets

200

(56)   **References Cited**

U.S. PATENT DOCUMENTS

2003/0028451 A1*	2/2003	Ananian	.... 705/27
2003/0182207 A1	9/2003	Skinner	
2005/0220326 A1	10/2005	Sim	
2005/0254714 A1	11/2005	Anne	
2006/0006224 A1	1/2006	Modi	
2007/0124211 A1	5/2007	Smith	
2008/0147883 A1	6/2008	Philyaw	
2008/0195536 A1	8/2008	Karns	
2008/0210754 A1*	9/2008	Lovett	.... 235/380
2009/0112768 A1	4/2009	Hammad	
2009/0200371 A1*	8/2009	Kean et al.	.... 235/379
2009/0234773 A1	9/2009	Hasson	
2009/0254485 A1	10/2009	Baentsch	
2010/0009663 A1	1/2010	Chang	
2010/0155470 A1	6/2010	Woronec	
2011/0099057 A1	4/2011	Tenyer	
2011/0251910 A1	10/2011	Dimmick	
2012/0099780 A1*	4/2012	Smith et al.	.... 382/136

* cited by examiner

FIG. 1

USER SELECTS DIGITAL WALLET AS PAYMENT
AT A CENTRAL SERVER
205

CENTRAL SERVER PROMPTS USER FOR
AUTHENTICATION
210

USER SELECTS BARCODE AS MEANS OF
AUTHENTICATION
215

CENTRAL SERVER INVOKES BARCODE
READER ON USER'S MOBILE DEVICE
220

USER CAPTURES IMAGE OF BARCODE
WITH A CAMERA IN THE MOBILE DEVICE
225

MOBILE DEVICE TRANSMITS BARCODE
DATA GENERATED BY THE MOBILE DEVICE
TO THE CENTRAL SERVER
230

CENTRAL SERVER DECRYPTS AND/OR DECODES
THE BARCODE DATA, IDENTIFIES THE MOBILE
DEVICE NUMBER, AND SENDS A ONE-TIME
PASSWORD TO THE MOBILE DEVICE
235

USER PROVIDES ONE-TIME PASSWORD TO
THE CLIENT COMPUTER, AND THE CLIENT
COMPUTER TRANSMITS THE PASSWORD
TO THE MERCHANT SERVER, AND TO THE
PAYMENT PROCESSING NETWORK
240

CENTRAL SERVER INITIATES PAYMENT
TRANSACTION
245

200

FIG. 2

FIG. 3

MERCHANT INVOKES PAYMENT
APPLICATION ON A MOBILE DEVICE
405

MERCHANT PROVIDES AMOUNT AND
TRANSACTION DETAILS TO THE MOBILE DEVICE
AND REQUESTS PAYMENT FROM USER
410

USER PRODUCES BARCODE AS MEANS OF
PAYMENT
415

MERCHANT CAPTURES IMAGE OF A BARCODE
WITH A CAMERA IN THE MOBILE DEVICE
420

MOBILE DEVICE TRANSMITS THE IMAGE TO
THE CENTRAL SERVER
425

CENTRAL SERVER INITIATES PAYMENT
TRANSACTION
430

400

FIG. 4

ISSUER
535

ISSUER
540

PAYMENT
PROCESSING
NETWORK
530

MOBILE
GATEWAY
525

SENDER
515

MOBILE DEVICE
520

SENDER'S
ACCOUNT
NUMBER
520(A)

RECIPIENT
505

PHYSICAL
PAYMENT TOKEN
510

BARCODE
510(A)

500

FIG. 5

SENDER REQUESTS CARD INFORMATION
FROM RECIPIENT
605

RECIPIENT PROVIDES BARCODE ON THEIR
PAYMENT CARD
610

SENDER CAPTURES IMAGE OF A BARCODE
WITH A CAMERA IN THE MOBILE DEVICE
615

MOBILE DEVICE GENERATES BARCODE DATA
FROM THE IMAGE OF THE BARCODE
620

MOBILE DEVICE TRANSMITS RECIPIENT'S
BARCODE DATA AND SENDER'S PAYMENT
CARD INFORMATION TO THE CENTRAL SERVER
625

CENTRAL SERVER INITIATES PAYMENT
TRANSACTION
635

600

FIG. 6

ISSUER 755

ISSUER 710

PAYMENT PROCESSING NETWORK 750

SENDER 705

PAYMENT SERVICE COMPUTER 715

WEBSITE 715(A)

INTERNET 720

MOBILE GATEWAY 735

CLIENT COMPUTER 725

MOBILE DEVICE 740

PHYSICAL PAYMENT TOKEN 745

BARCODE 745(A)

RECIPIENT 730

700

FIG. 7

SENDER NOTIFIES CENTRAL SERVER THAT FUNDS
ARE AVAILABLE TO TRANSFER AND SENDS
FUNDS TO ISSUER
805

CENTRAL SERVER NOTIFIES RECIPIENT THAT
FUNDS ARE AVAILABLE TO BE CLAIMED AND
PROVIDES AN AUTHENTICATION CODE
810

RECIPIENT PROVIDES AUTHENTICATION CODE
TO CENTRAL SERVER FOR AUTHENTICATION
815

RECIPIENT INVOKES BARCODE READER AND
P2P APPLICATION ON RECIPIENT'S MOBILE DEVICE
820

RECIPIENT CAPTURES IMAGE OF A BARCODE
WITH A CAMERA IN THE MOBILE DEVICE
825

MOBILE DEVICE GENERATES BARCODE DATA
FROM THE IMAGE OF THE BARCODE
830

P2P APPLICATION RETRIEVES RECIPIENT'S
PAYMENT CARD INFORMATION REQUIRED
FOR THE TRANSFER
835

MOBILE DEVICE TRANSMITS BARCODE DATA
AND RECIPIENT'S PAYMENT CARD INFORMATION
TO THE CENTRAL SERVER
840

CENTRAL SERVER INITIATES PAYMENT
TRANSACTION AND RECIPIENT'S PAYMENT
CARD RECEIVES THE TRANSFER OF FUNDS AT THE
ISSUER
845

800

FIG. 8

ANTENNA

945

CAMERA

905

PROCESSOR
910

DISPLAY
915

DATA INPUT/OUTPUT/IMAGE
CAPTURE AND PROCESSING
920

COMMUNICATIONS
925

APPLICATIONS/DATA STORAGE/
MEMORY
930

CONTACTLESS ELEMENT
INTERFACE
935

CONTACTLESS ELEMENT
SECURE MEMORY/NFC/WIFI DATA
TRANSFER
940

900

FIG. 9

1005

1030

1015

Payment Account Number (BIN/PAN format)
NNNNNNNNNNNNNNNN

1010

1020

Name of Consumer

Expiration Date

1025

BAR-CODE, DECAL, IMAGE
(REPRESENTING PAYMENT ACCOUNT
AND/OR CONSUMER DATA)

FIG. 10A

1055

BAR-CODE, DECAL, IMAGE
(REPRESENTING PAYMENT ACCOUNT
AND/OR CONSUMER DATA)

1050   **FIG. 10B**

FIG. 11

FIG. 12

METHOD FOR USING BARCODES AND MOBILE DEVICES TO CONDUCT PAYMENT TRANSACTIONS

CROSS-REFERENCES TO RELATED APPLICATIONS

The present application is a non-provisional application of and claims priority to U.S. Provisional Application No. 61/526,969, filed on Aug. 24, 2011, the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND

Embodiments of the invention are directed to systems, apparatuses and methods for conducting payment transactions and processing data related to such transactions.

Conventional card present payment transactions often begin with a user taking a payment card, and then swiping the payment card in a payment card terminal to initiate a transaction. Such transactions may not be particularly secure if an unauthorized person has somehow obtained the payment card.

Conventional card not present payment transactions often begin with a user taking a payment card, and then inputting his card number into a checkout page on a Web site. Such transactions may also not be particularly secure, if the information on the card is somehow obtained by an unauthorized user. Further, the need to manually enter data into the checkout page is time consuming and inconvenient.

Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

Embodiments of the invention are directed to systems, apparatuses and methods that can utilize mobile devices (e.g., smart phones) and physical payment tokens with two dimensional barcodes to conduct payment transactions.

Consumer payment devices are used to conduct transactions to pay for goods or services by people every day and all over the world. Some common payment devices are credit cards and debit cards. One advantage of using such payment devices is that the transaction processing infrastructure has been developed and implemented based on using these types of payment devices so that the process of initiating, authorizing, settling, and clearing a payment transaction is straightforward and relatively well understood by consumers, merchants, and issuers.

However, although credit cards and debit cards are the most commonly used consumer payment devices at present, they may not be optimal for conducting payment transactions in ways that are becoming of greater interest to consumers. For example, consumers are growing increasingly interested in conducting payment transactions using mobile devices such as smart phones. For some of these devices the standard ways of providing account information, authentication information, or other data used to conduct a payment transaction may not be practical or desirable to use. For example, data entry using a keyboard or keypad can be difficult and prone to errors when using many mobile devices. Further, although technologies have been developed to enable greater use of mobile devices to conduct payment transactions (such as embedded chips and contactless communications methods), consumers may not be as familiar or as comfortable using these technologies as they are with a credit card or debit card-based transaction system. This may be especially prevalent in pay-

ment transactions with online merchants, small merchants, personal payments, and person-to-person ("P2P") payment transfers.

In order to increase the adoption and use by consumers of mobile payment technologies and address the interest of consumers in being able to conduct payment transactions using mobile devices, embodiments of the invention can integrate parts of a card-based transaction processing infrastructure with mobile devices in a way that does not introduce significant new hardware capability or over-the-air software provisioning as in the case of NFC technologies. Further, the methods of conducting payment transactions using these devices takes into account the capabilities and relative advantages of such devices.

Embodiments of the invention facilitate the use of mobile devices for making payments for goods and services by integrating the image capture and image processing capabilities of certain mobile devices with the existing card-based payment transaction infrastructure and processes that are familiar to consumers, merchants, and issuers. In some embodiments, a camera contained in a mobile device (such as a smart phone, generic mobile phone, or PDA) is used to capture an image of a two-dimensional barcode that is visible on the surface of a substrate (such as a consumer payment device in the form of a card, e.g., a credit card, debit card, or prepaid card). The substrate may be part of a physical payment token. The barcode may represent or otherwise encode one or more of payment account data, consumer authentication data, consumer profile data, or other relevant information. In some embodiments, the captured image may be processed by the mobile device to extract the payment account data, authentication data, or other relevant data. This data may then be communicated to a data processing element that is connected to, or forms part of, a payment processing network in order to conduct the desired payment transaction.

One embodiment of the invention is directed to a method of conducting a payment transaction comprising: capturing an image of a two-dimensional barcode on a physical payment token with a camera in a mobile device; generating barcode data based on the captured image; and transmitting the barcode data to a central server computer, wherein the central server computer initiates the payment transaction.

Another embodiment of the invention is directed to a mobile device comprising a processor; a camera coupled to the processor; and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for implementing a method comprising; capturing an image of a two-dimensional barcode on a physical payment token with the camera; generating barcode data based on the captured image, and transmitting the barcode data to a central server computer, wherein the central server computer initiates the payment transaction.

Another embodiment of the invention is directed to a method of conducting a payment transaction comprising: receiving barcode data, wherein an image of a two-dimensional barcode on a physical payment token is captured with a camera in a mobile device, and wherein the barcode data is based on the captured image; and initiating a payment transaction by the central server computer with the barcode data.

Another embodiment of the invention is directed to a server computer comprising a processor; and a computer readable medium coupled to the processor, the computer readable medium comprising code, for executing a method comprising: receiving barcode data, wherein an image of a two-dimensional barcode on a physical payment token is captured with a camera in a mobile device, and wherein the barcode

data is based on the captured image; and initiating a payment transaction with the barcode data.

Further details regarding embodiments of the invention can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a block diagram of a system according to an embodiment of the invention. The system can be used to conduct an online transaction with a separate client computer.

FIG. 2 shows a flowchart illustrating a method that can be used with the system in FIG. 1.

FIG. 3 shows a block diagram of a system another embodiment of the invention. The system can be used to conduct a face-to-face payment transaction.

FIG. 4 shows a flowchart illustrating a method that can be used with the system in FIG. 3.

FIG. 5 shows a block diagram of a system according to another embodiment of the invention. The system can be used to implement a person-to-person ("P2P") payment transaction. The sender and recipient of the funds are face-to-face.

FIG. 6 shows a flowchart illustrating a method that can be used with the system in FIG. 5.

FIG. 7 shows a block diagram of a system according to an embodiment of the invention.

FIG. 8 shows a flowchart illustrating a method that can be used with the system in FIG. 7.

FIG. 9 is a block diagram illustrating certain elements of a mobile device that may be used to implement an embodiment of the invention.

FIG. 10(a) shows a drawing of a payment card with a barcode on it.

FIG. 10(b) shows a block diagram of a consumer payment device that includes a barcode or decal representing information that may be used in conducting a payment transaction using an embodiment of the invention.

FIG. 11 shows a block diagram illustrating elements of a system that may be operated to implement an embodiment of the invention.

FIG. 12 shows a number of exemplary two-dimensional barcodes.

DETAILED DESCRIPTION

One embodiment of the invention is directed to a method of conducting a payment transaction. The method comprises capturing an image of a two-dimensional barcode on a physical payment token such as a credit card with a camera in a mobile device. After the image of the two-dimensional barcode is captured, the mobile phone can generate barcode data based on the captured image. The barcode data may be data representing an actual image of the barcode (e.g., in a JPEG file) or may be data that is encoded by the barcode. For example, with respect to the latter embodiment, the barcode data may be a PAN or primary account number that the barcode actually represents.

Once the barcode data is obtained, it may be transmitted to a central server computer. The central server computer may be in a payment processing network, or in any other suitable location.

The central server computer then initiates the payment transaction using the barcode data. As explained in detail below, the transaction may be initiated in a number of different ways. In some embodiments, the transaction may be initiated depending upon the role of the user that is associated with the barcode. For instance, in some embodiments, if the sender of funds uses his mobile device to capture the barcode

associated with the sender, then the transaction may be initiated by sending the sender a dynamic account identifier, which can be input into an electronic shopping cart. If the recipient of funds is using his mobile device to capture the two-dimensional barcode associated with the sender, then the transaction may be initiated by an authorization request message to an issuer associated with an account number associated with the sender.

In some embodiments, after the barcode data is received by the server computer, the server computer may then transmit account holder data back to the mobile device. The mobile device may receive this data, and may then display the data. For example, account holder data such as a name, address, card number, etc. may be sent back to the mobile device after the mobile device scans the barcode on the physical payment token.

Prior to discussing embodiments of the invention, a further description of some terms may be helpful in understanding embodiments of the invention.

A "two-dimensional barcode" may include an optical machine-readable representation of data, which has at least two dimensions. One type of barcode is a QR CODE® (quick-response code). A QR CODE® two-dimensional code (trademark registered to Denso Corp. of Tokyo, Japan) is a printable, machine-readable code that has become widely popular with advertisers and consumers. Two-dimensional barcodes may comprise any suitable types of patterns including rectangles, dots, hexagons, and other geometric patterns in two dimensions. Two-dimensional barcodes may also have any suitable dimensions. For example, suitable two-dimensional barcodes may have a length and/or width less than about 3 inches, 2 inches, or 1 inch. Examples of two-dimensional barcodes are shown in FIG. 12.

In some embodiments, two-dimensional barcodes may be generated using different algorithms. Unlike one dimensional barcodes (e.g., UPCs or universal product codes), the additional dimension provided by two-dimensional barcodes allows them to be encoded in different ways. For example, in embodiments of the invention, a first issuer may use a first barcode generation process that utilizes a combination or rectangles and dots to form a first issuer specific barcode. Combinations of these rectangles and dots may be used encode hundreds of different PANs for that first issuer's account holders. A second issuer may use a second barcode generation process that utilizes a combination or hexagons and dots to form a second issuer specific barcode. Combinations of these hexagons and dots may be used encode hundreds of different PANs for that second issuer's account holders.

Two-dimensional barcodes can provide additional security over traditional one-dimensional barcodes. For instance, if a payment card with a two-dimensional barcode encoding a PAN according to the first issuer specific encoding process is stolen or somehow illegally obtained, and if the first issuer specific algorithm is somehow determined by the unauthorized entity, there is no risk that the second issuer specific algorithm is compromised since the first and second issuer specific algorithms are distinct.

The two-dimensional barcodes may encode any suitable data. Such data may include data that can be present on a typical payment card. Such data may include an account number, a card verification value, an expiration date, a service code, etc. It may also encode other personal information such as an electronic communication address (e.g., a phone number, e-mail address or IP address), a physical address (e.g., home address), or personal identification information (e.g., a

5

social security number), or preferences (e.g., a preference for aisle seats when booking an airplane ticket).

"Barcode data" may include any suitable type of data relating to a barcode. Barcode data may include data representing account holder (e.g., cardholder data) including a primary account number, a shipping address, a phone number, seating preferences, etc. The data representing the account holder that can be encoded as a barcode may be in the clear if decoded, or may be an encrypted value. For example, a real account number such as 1122334455667788 may be encoded as a two-dimensional barcode. Alternatively, an encrypted version of this number such as 1838527839287861 may be encoded as a two-dimensional barcode. Encrypted data representing the account holder provides for an extra level of security. Barcode data may also include data that represents an image of a barcode. For example, in some embodiments, barcode data may comprise a JPEG or GIF file with data that can be used to form an image of a barcode.

A "physical payment token" can include any suitable physical device that can be associated with a payment transaction. In some cases, the physical payment token may have an additional memory or computer readable storage medium which stores account holder data such as a PAN, CVV (card verification value), service code, expiration date, shipping address, and other information. Suitable physical payment tokens can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, credit or debit cards (with a magnetic stripe), keychain devices (such as the Speedpass® commercially available from Exxon-Mobil Corp.), and key fobs. The physical payment tokens can be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

A "mobile device" can be any device that can allow a user to communicate with another entity. Examples of mobile devices include mobile communication devices such as phones (e.g., cellular phones, smart phones, etc.). Typically, a mobile device according to an embodiment of the invention includes a processor, a computer readable medium coupled to the processor, and a camera coupled to the processor. Further details regarding specific mobile devices are provided below.

As used herein, a "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

In some embodiments, a server computer may comprise a computer readable medium coupled to the processor. The computer readable medium comprises code, for executing a method comprising: receiving barcode data, wherein an image of a two-dimensional barcode on a physical payment token is captured with a camera in a mobile device, and wherein the barcode data is based on the captured image; and initiating a payment transaction with the barcode data.

"Account holder data" can include information about an account holder. The account holder can possess a payment card or other physical payment token that is issued by an issuer.

6

A "payment processing network" may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet®. Payment processing networks such as VisaNet® are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet®, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

An "authorization request message" may include a message, or sequence of messages, that requests an issuer of a payment account to authorize a transaction. An authorization request message according to an embodiment of the invention may comply with ISO (International Organization for Standardization) 8583, which is a standard for systems that exchange electronic transactions made by cardholders using payment cards. Authorization request messages may comprise an account number, a transaction amount, a CVV (card verification value), expiration date, service code, and other information.

An "authorization response message" may refer to a message, or sequence of messages, that responds to a merchant's and/or acquirer's request to authorize a transaction. An authorization response message according to an embodiment of the invention may comply with ISO 8583, which, as described above, is a standard for systems that exchange electronic transactions made by cardholders using payment cards. Authorization response messages may comprise authorization codes for authorized transactions.

FIG. 1 shows a block diagram of a payment processing system according to an embodiment of the invention. It can be used to perform an online payment.

FIG. 1 shows a system 100 including a user 105, who can use a client computer 110 to communicate with a merchant server computer 135 via the Internet 130 or other communication medium. The merchant server computer 135 may be operatively coupled to an issuer computer 150, operated by an issuer, via an acquirer computer 140, operated by an acquirer, and a payment processing network 145. The payment processing network 145 may store a digital wallet 145(a). While the digital wallet 145(a) is shown as being within the payment processing network 145, it could be outside of the payment processing network 145 in other embodiments of the invention. The digital wallet 145(a) may contain various pieces of information of the user 105 such as account numbers associated with different issuers.

The user 105 may also use a mobile device 115 to communicate with the payment processing network 145 via a mobile gateway 125. In this embodiment, the mobile device 115 may be a mobile phone.

The user 105 may also have a physical payment token 120, which may comprise a two-dimensional barcode 120(a). The physical payment token 120 could be in the form of a payment card.

In some embodiments, the issuer operating the issuer computer 150 or the payment processing network 145 may distribute the physical payment tokens with two-dimensional barcodes prior to any transactions being conducted. Thus, if the barcodes encode encrypted primary account numbers or other sensitive information, they can be decrypted with keys residing at the issuer computer 150 or the payment processing network 145.

Methods according to embodiments of the invention can be described with reference to FIGS. 1 and 2.

7

8

In a typical purchase transaction, a user **105** can use the client computer **110** to contact the merchant Website **135**(*a*) on the merchant server computer **135** via the Internet **130**. When the user **105** finds a good or service to purchase on the Website **135**(*a*), the user **105** can proceed to the checkout page on the merchant's Website **135**(*a*). At the checkout page, the user **105** can be presented with a number of different payment options including a digital wallet payment option.

The digital wallet **145**(*a*) may be programmed to maintain an association between one or more payment accounts (such as a bank account or credit card account) in a digital wallet database. Further details regarding digital wallets can be found in U.S. Patent Application No. 61/466,409 filed on Mar. 22, 2011, which is incorporated herein by reference in its entirety.

FIG. **2** shows a flowchart illustrating a method that can be used with the system in FIG. **1**. The method **200** may begin at step **205** when the user **105** selects the digital wallet payment option and may access the digital wallet **145**(*a*) via the merchant Website **135**(*a*) by providing user credentials such as a user ID and a password. After the user **105** selects the digital wallet option, the digital wallet **145**(*a*) may attempt to authenticate the user **105** and provide the user with a number of authentication options (step **210**) including a barcode authentication option.

The user **105** may select the barcode authentication option (step **215**). If the user selects the barcode authentication option, the digital wallet can invoke an application stored on the mobile device **115**. This can be done by communicating with the user's mobile device **115** (step **220**) via the mobile gateway **125**. The digital wallet **145**(*a*) may have previously stored the phone number (or other identifier such as an IP address) associated with the mobile device **115**.

In step **225**, the user **105** can use the camera on the user's mobile device **115** to capture an image of the barcode **120**(*a*) on the physical payment token **120**. The mobile device **115** may be configured to capture an image of a two-dimensional barcode **120**(*a*) on the physical payment token **120** with a camera in the mobile device **115**, generate barcode data based on the captured image, and transmit the barcode data to a central server computer such as a server computer residing in the payment processing network **145**. The server computer in the payment processing network **145** can then initiate the payment transaction.

In step **230**, the mobile device **115** can transmit the barcode data to the mobile gateway **125** and then to the payment processing network **145**. After the barcode data is transmitted from the mobile device **115**, the server computer in the payment processing network **145** can receive the barcode data. The server computer may decode the barcode data if data representing an image of the barcode is received. Alternatively, it may decrypt the data if the image of the barcode representing an encrypted value was previously decoded by the mobile device **115**. In other embodiments, the server computer may receive the decoded barcode information in the clear. For instance, the mobile device **115** may decode the barcode data to generate a primary account number, and that primary account number associated with the user may be transmitted to and received by the server computer.

In step **235**, once the barcode data is received by the central server computer in the payment processing network **145**, the barcode data is decoded if it has not been previously decoded by the mobile device **115**. Further, if the information (e.g., primary account number) associated with the barcode **120**(*a*) was previously encrypted, the server computer may decrypt the information using an appropriate key. The decrypted and/or decoded information may include the mobile device num-

ber. In some embodiments, the mobile device number may be obtained using, for example, an account number that was obtained from the barcode data. The server computer in the payment processing network **145** may then transmit a one-time password to the mobile device **115**. Alternatives to the one-time password include DCVVs (dynamic verification values) and one-time account numbers.

In step **240**, the user **105** may then input the one-time password into the client computer **110** and this may be transmitted to the payment processing network **145** via the Internet **130** and the merchant server computer **135**.

If the one-time password that is received at the payment processing network **145** is the same as the one that was previously generated by the payment processing network **145**, then the user **105** can be authenticated, and the payment transaction may be initiated (step **245**). The user **105** is authenticated, because he has provided the user ID and password to access the digital wallet **145**(*a*), provided the correct one-time password, and was in possession of the authentic physical payment token **120** as well as the authentic mobile device **115**. Embodiments of the invention are more secure than conventional card present and card not present payment processes, since multiple factors of authentication are used in embodiments of the invention.

In some embodiments, the payment processing network **145** may initiate the transaction by generating an authorization request message for the transaction. The authorization request message may be sent to the issuer computer **150**. After the issuer computer **150** receives the authorization request message, the issuer computer **150** may generate and send an authorization response message to the payment processing network **145** indicating whether or not the transaction was approved. The payment processing network **145** may transmit the authorization response message to the acquirer computer **140**, and then to the merchant server computer **135**.

Although the transaction described herein is in the context of an online purchase transaction involving a merchant, the transaction may also be an automated teller machine (ATM) transaction or conducted in person at a physical point of sale (POS) terminal. Thus, the merchant server computer **135** as shown in FIG. **1** and described herein may alternatively be an ATM or POS terminal in other embodiments of the invention.

FIG. **3** shows a block diagram of a system according to an embodiment of the invention. The system can be used for face-to-face payment transactions.

FIG. **3** shows a system **300** including a user **305** and a merchant **315**. The merchant **315** may be a mobile merchant (e.g., a food truck) or a stationary merchant. The user **105** may have a physical payment token **120** comprise a two-dimensional barcode **120**(*a*).

The merchant **315** may operate a mobile device **320**, which communicates with the payment processing network **330**, an issuer computer **340**, and acquirer computer **335** via a mobile gateway **125**. The acquirer computer **335** may also hold an account of the merchant **315**.

FIG. **4** shows a flowchart illustrating a method according to an embodiment of the invention. The method **400** can be described with reference to FIG. **3**.

The method may begin with the user **305** selecting items for purchase at the merchant **315**.

In step **405**, the merchant invokes a payment application on the mobile device **320**. In step **410**, the merchant **315** provides the amount of the transaction and any transaction details to the mobile device **320**. Other suitable transaction details may comprise descriptions of the items purchased. The merchant **315** may then request that the user **305** present the physical payment token **310** with the barcode **310**(*a*).

At step **415**, the user **315** provides a physical payment token **310** with the barcode **310**(*a*) to the merchant **315**. The physical payment token **310** may be payment card or a mobile phone. If the physical payment token **310** is in the form of a card, the two-dimensional barcode **310**(*a*) may be imprinted on the card or may be in the form of a sticker on the card. If it is in the form of a mobile phone, then the barcode **310**(*a*) may be shown on a screen in the mobile phone.

At step **420**, the merchant captures the image of the barcode **310**(*a*) with the camera in the mobile device **320**, and the mobile device **320** generates barcode data from the barcode **310**(*a*).

At step **425**, the mobile device transmits the barcode data to a central server computer in the payment processing network **330**, via the mobile gateway **325**.

At step **430**, the central server computer in the payment processing network **330** initiates the payment transaction.

The server computer in the payment processing network **330** may initiate the transaction by generating an authorization request message for the transaction. The server computer may either decode and/or decrypt the barcode data to determine information including a primary account number, service code, card verification value, expiration date, etc. The server computer may then format the authorization request message as described above.

Once generated, the authorization request message may be sent to the issuer computer **340**. After the issuer computer **340** receives the authorization request message, the issuer computer **340** may analyze the authorization request message and may determine if the transaction is authorized or not. After this determination, the issuer computer **340** may generate and send an authorization response message to the payment processing network **330** indicating whether or not the transaction was approved. The payment processing network **330** may transmit the authorization response message to the acquirer computer **335**, and then to the merchant **315**. Alternatively, the payment processing network **330** may transmit the authorization response message to the mobile device **320**.

At a later time, a clearing and settlement process may occur between the issuer computer **340** and the acquirer computer **335**.

FIG. **5** shows a block diagram of a system according to an embodiment of the invention. The system **500** may implement a person-to-person payment transaction when the sender and recipient of the funds can be face-to-face.

FIG. **5** shows a recipient of funds **505** and a sender of funds **515** at the same location. The recipient **505** may have a physical payment token **510** with a barcode **510**(*a*) on it. The sender **515** may have a mobile device **520**, which may store the sender's account number **520**(*a*). In other embodiments, the mobile device **520** need not store the sender's account number **520**(*a*). For example, in other embodiments, the sender's account number may be stored at the payment processing network **530** and may be determined after the payment processing network **530** receives the mobile device **520** identifier associated with the mobile device **520**. The mobile device **520** may be in operative communication with a payment processing network **530**, a first issuer computer, and a second issuer computer via a mobile gateway **525**. The first issuer computer may be associated a first issuer **535** that issued the account number encoded by the barcode **510**(*a*) on the physical payment token **510**. The second issuer computer may be associated with a second issuer **540** that issued the sender's account number **520**(*a*).

FIG. **6** shows a flow diagram of an embodiment of a typical payment transaction implemented with the system in FIG. **5**.

The method **600** may begin at step **605** when the recipient **505** seeks payment from the sender **515**, and requests payment card (or other form factor) information from the recipient **505**.

At step **610**, the recipient **505** presents his physical payment token **510** to the sender **515**. As described above, the physical payment token **510** may be in the form of a card, phone, or other suitable form factor.

At step **615**, the sender captures the image of a barcode **510**(*a*) with the camera in the mobile device **520**. Once captured, the mobile device **520** generates the barcode data associated with the barcode **510**(*a*) in step **620**.

At step **625**, the mobile device **520** transmits the recipient's barcode data, the transaction amount, and sender's account number or a mobile device identifier to the central server computer in the payment processing network **530** via the mobile gateway **525**.

At step **635**, the central server computer in the payment processing network **530** initiates the payment transaction. The central server computer in the payment processing network **530** can decode and/or decrypt the barcode data if the received barcode data has not been previously decoded or decrypted. The central server computer has the sender's account number (which may be derived from the sender's mobile device identifier if the mobile device identifier and the sender's account number are stored at the payment processing network **530**), the amount to be transferred from the sender's account to the recipient's account, and the recipient's account number from the barcode data.

The server computer in the payment processing network **530** may then initiate the transaction by generating appropriate payment authorization messages to the first and second issuers **535**, **540** (or to their respective computers). In some embodiments, an OCT (original credit transaction) message may be sent to credit the account of the recipient **505** at the first issuer **535**, while an AFT (account funding transaction) message may be sent to the second issuer **540** to debit the account of the sender **515**.

An AFT (Account Funding Transaction) is a transaction designed to supply funds to another account such as a credit, prepaid, debit, ATM or on-line account. In some embodiments, the AFT message can be used to pay a service provider for sending funds to the recipient and results in a debit to the sender's account. The amount of the debit can be the amount of the credit to be delivered to the recipient plus any fees being charged by the service provider such as a transfer fee, or a currency conversion fee (if applicable).

An AFT indicator can be used in both the authorization and clearing and settlement transactions and is preceded by an authorization. Settlement can take place within two working days, or more or less than this. Neither the authorization nor the clearing transaction carries any financial information about the recipient of a money transfer. In some embodiments, the AFT carries the account number or other identifier associated with the payment account of the sender. An AFT message can also accompanied by indicators, which allow the sender's issuer to take appropriate authorization decisions. Indicators include channel information such as Mail Order/Telephone Order or Internet, etc.

The following fields can be used for an AFT and can be supported in messages and clearing and settlement transactions. The fields included in a traditional AFT message can include, but is not limited to an account number, a processing code; merchant type; CAVV result code; Mail Order/Telephone Order/Electronic Commerce Indicator; Mail/Phone/Electronic Commerce Indicator; transaction ID (XID); etc.

11   12

An OCT (Original Credit Transaction) is typically a clearing and settlement credit transaction designed for use in business applications such as a business money transfer or business-to-consumer repayments. In embodiments of the invention, the OCT can be used to deliver funds to the recipient account. It can be separate from, and can take place after, the AFT transaction. This timing can ensure that payment funds are secured before funds are sent to the recipient.

The amount of the OCT can be the amount agreed to by the sender and the service provider in the currency agreed. The OCT can carry the account number of the recipient and no information about the sender. A special indicator can identify an OCT to the recipient's issuer bank. Settlement can take place within two days, or more or less time than this.

At a later time, a clearing and settlement process may occur between the first and second issuers 535, 540 via the payment processing network 530.

FIG. 7 shows a block diagram of a system according to an embodiment of the invention. It can be used to implement a person-to-person payment transaction when the sender and recipient of the funds are not face-to-face.

The system 700 includes a recipient 730, who can use a client computer 725 to communicate with a payment service computer 715 via the Internet 720 or other communication medium. The payment service computer 715 may be operatively coupled to a first issuer 755, and a second issuer 710 via a payment processing network 750.

The recipient 730 may also use a mobile device 740 to communicate with the payment service computer 715 comprising a Website 715(a) via a mobile gateway 735. The recipient 730 may also have a physical payment token 745, which may comprise a two-dimensional barcode 745(a).

The sender 705 may also communicate with the payment service computer 715 (by operating a client computer, not shown), and may have relationship with the issuer operating the issuer computer 710.

FIG. 8 shows a flowchart illustrating a method that can be described with reference to the system in FIG. 7.

The method 800 may begin at step 805 when a sender 705 wants to transfer funds to the recipient 730.

At step 810, the payment service computer 715 can notify the recipient 730 at his mobile device 740 via the mobile gateway 735 that funds are available to be claimed and provides the recipient 730 with a claim code. The notification could be in the form of a text message or an e-mail.

At step 815, the recipient 730 may contact a Website 715(a) operated by the payment service computer 715 using the client computer 725. Once on the Website 715(a), the recipient 730 may provide the claim code to the payment service computer 715. The Website 715(a) may then provide a screen requesting that the recipient 730 to choose a mode of entering his payment card information (e.g., for receiving the transfer of funds).

At step 820, the recipient 730 may choose to enter his payment card information by using a barcode, and invoke the person-to-person ("P2P") payment application on the mobile device 740. Then, at step 825, the recipient 730 can capture an image of the barcode 745(a) with a camera in the mobile device 740.

At step 830, the mobile device 740 generates barcode data from the image of the barcode 745(a). At step 835, the P2P application may retrieve the recipient's payment card (or other form factor) information required for the transfer.

At step 840, the mobile device 740 transmits the barcode data to the payment service computer 715, which transmits it to the payment processing network 750. As described above, the barcode data may be decoded if it the barcode has not previously been decoded. The barcode data may also be decrypted if the barcode previously represented an encrypted value.

At step 845, the payment processing network 750 initiates the payment transaction. The server computer in the payment processing network 750 has the account number of the recipient 730, the account number of the sender 705, and the amount to be transferred from the sender 705 to the recipient.

The server computer in the payment processing network 750 may initiate the transaction by generating and sending appropriate payment instruction messages to the first and second issuers 755, 710 (or to their respective computers). In some embodiments, an OCT (original credit transaction) message may be sent to credit the account of the recipient 730 at the first issuer 755, while an AFT (account funding transaction) message may be sent to the second issuer 710 to debit the account of the sender 705. AFT and OCT transactions and message are described above, and need not be repeated here.

FIG. 9 is a block diagram illustrating certain elements of a mobile device that may be used to implement an embodiment of the invention. As shown, the mobile device 900 may include a processor 910 or processing element that executes instructions or code in order to implement functions, operations, methods, or processes. The mobile device may also include a camera 905 (or other form of image capture element), a display 915, data input means 920 (a keypad, touch screen, track ball), data output means (the display, a speaker), image capture and processing capabilities, communications elements 925 to enable the exchange of messages, signals, and data between the mobile device and a cellular network or POS terminal, a set of instructions or code for executing one or more applications (for initiating a payment transaction, processing an image, etc.) and/or data stored in a memory 930, a contactless element interface 935 (if applicable), a contactless element 940 (which may include a secure data storage element and a data transfer element) and an antenna 945 for transmitting data, signals, or other information from the mobile device.

The memory 930 may comprise a computer readable medium comprising code, executable by the processor 910 for implementing a method comprising; capturing an image of a two-dimensional barcode on a physical payment token with the camera; generating barcode data based on the captured image, and transmitting the barcode data to a central server computer. The memory 930 may also store encryption keys for decrypting any encrypted values that are decoded from the barcodes being scanned.

FIG. 10(a) is a diagram illustrating an example of a physical payment token device that includes a barcode or decal representing information that may be used in conducting a payment transaction using an embodiment of the invention, and FIG. 10(b) is a diagram illustrating another format in which the barcode or decal may be provided.

As shown in FIG. 10(a), a physical payment token 1005 may take the form of a card or substrate (e.g., a credit card, debit card, or prepaid card) having a front side or surface on which contains embossed or printed information. The information may include the consumer name 1010, the payment account number 1015 (typically in a standard form that includes an identification of a BIN and PAN), an expiration date of the payment device 1020, and an image, barcode, or decal 1025 that represents or otherwise encodes data or information relevant to conducting a payment transaction (such as the payment account number, the consumer authentication data, like a PIN, and other data that may be relevant to conducting a payment transaction). The information may also include a signature panel and CVV2 square. The back side or

surface may include a magnetic stripe **1030** in which is encoded payment account and other data. Other new information and non-payment information may be contained on the physical payment token **1005** as well. In an embodiment, information from the front of the card or the back of the card can be printed or embossed on the back of the card or the front of the card, respectively.

As shown in FIG. **10**(*b*), a physical payment token **1050** may include the image, barcode, or decal **1055** that represents or otherwise encodes data or information relevant to conducting the payment transaction may also be provided in another format, such as placed on a different type of substrate (e.g., a card, paper, stamp, key fob, etc.).

The various participants and elements described herein may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in the above-described Figures, including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

FIG. **11** is a block diagram of elements that may be present in a computing device or system configured to execute a method, process, function, or operation in accordance with some embodiments of the invention. The subsystems shown in FIG. **11** are interconnected via a system bus **575**. Additional subsystems such as a printer **574**, a keyboard **578**, a fixed disk **579**, a monitor **576**, which is coupled to a display adapter **582**, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller **571**, can be connected to the computing system by any number of means known in the art, such as a serial port **577**. For example, the serial port **577** or an external interface **581** can be used to connect the computing device to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via the system bus **575** allows a programmed central processor **573** (e.g., a microprocessor, CPU, etc.) to communicate with each subsystem and to control the execution of instructions that may be stored in a system memory **572** or the fixed disk **579**, as well as the exchange of information between subsystems. The system memory **572** and/or the fixed disk **579** may embody a computer-readable medium.

A number of advantages of embodiments of the invention are described above. Other advantages also exist. For example, because payment card or account information does not reside in a digital wallet or in the "cloud," it is difficult for an unauthorized person to steal the payment card or account number by hacking computer systems that might otherwise store this information. As noted above, the payment card and account information can be stored in a two-dimensional barcode on a physical payment token. The consumer has the convenience of a digital wallet, without having to enter in card information, for example, into a computer during an online transaction.

As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably programmed computing device, microprocessor, data processor, or the like. The set of instructions or software code may be stored in a memory or other form of data storage element which is accessed by the computing device, microprocessor, etc. In other embodiments, the functions, processes, operations or method steps may be implemented by firmware or a dedicated processor, integrated circuit, etc.

It should be understood that the present invention as described above can be implemented in the form of control

logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer-readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art. For example, although the scanning of barcodes on physical payment devices is described in detail for the purpose of inputting payment account information into a payment system, embodiments of the invention can also be used for other purposes. For example, a physical payment token may include other information such as a shipping address, home address, preferences, family status, etc., and this information may be decoded and/or decrypted by a mobile device, and subsequently used in a transaction. In some cases, this information can be used to automatically form fill information on a Web page or other interface operated by a payment recipient (e.g., a merchant).

The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

What is claimed is:

1. A method of conducting a payment transaction comprising:

receiving, by a mobile device operated by a user, an authentication communication from a digital wallet of a central server computer, wherein the authentication communication is sent in response to the payment transaction being initiated by the user on a client computer;

capturing an image of a two-dimensional barcode on a physical payment token with a camera in the mobile device;

generating, by the mobile device, barcode data based on the captured image;

transmitting, by the mobile device, the barcode data to the central server computer comprising the digital wallet,

wherein the central server computer decrypts or decodes the barcode data from the mobile device; and

receiving, at the mobile device, a dynamic data element from the central server computer, wherein the dynamic data element is adapted to be transmitted to the central server computer from the client computer in which the user has entered the dynamic data element,

wherein the central server computer initiates the payment transaction after the central server computer determines that the dynamic data element received from the client computer matches the dynamic data element that was sent from the central server computer to the mobile device.

2. The method of claim 1 wherein the two-dimensional barcode encodes a primary account number.

3. The method of claim 2 wherein the primary account number is encrypted.

4. The method of claim 1 wherein the physical payment token is a card.

5. The method of claim 1 further comprising:

receiving account holder data from the central server computer, wherein the account holder data is associated with the barcode data; and

displaying the account holder data.

6. The method of claim 1 wherein the two-dimensional barcode encodes a card verification value, expiration date, or service code.

7. The method of claim 1 wherein the two-dimensional barcode encodes an electronic communication address, a physical address, personal identification information, or preferences of the user.

8. A mobile device comprising:

a processor;

a camera coupled to the processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for implementing a method comprising

receiving an authentication communication from a digital wallet of a central server computer, wherein the authentication communication is sent in response to the payment transaction being initiated by the user on a client computer,

capturing an image of a two-dimensional barcode on a physical payment token with the camera,

generating barcode data based on the captured image,

transmitting the barcode data to the central server computer comprising the digital wallet, wherein the central server computer decrypts or decodes the barcode data from the mobile device, and

receiving a dynamic data element from the central server computer, wherein the dynamic data element is adapted to be transmitted to the central server computer from the client computer in which the user has entered the dynamic data element,

wherein the central server computer initiates a payment transaction after the central server computer determines that the dynamic data element received from the client computer matches the dynamic data element that was sent from the central server computer to the mobile device.

9. The mobile device of claim 8 wherein the two-dimensional barcode encodes a primary account number.

10. The mobile device of claim 9 wherein the primary account number is encrypted, and wherein the method further comprises code for decrypting the primary account number.

11. The mobile device of claim 8 further wherein the mobile device further comprises an antenna coupled to the processor.

12. The mobile device of claim 8 further comprising:

a display coupled to the processor.

13. A method of conducting a payment transaction comprising:

sending, by a central server computer comprising a digital wallet, an authentication communication from the digital wallet to a mobile device, wherein the authentication communication is sent in response to the payment transaction being initiated by a user on a client computer;

receiving barcode data at the central server computer from the mobile device, wherein an image of a two-dimensional barcode on a physical payment token is captured with a camera in the mobile device, and wherein the barcode data is based on the captured image;

generating a dynamic data element when the barcode data is authenticated;

transmitting the dynamic data element to the mobile device;

receiving the dynamic data element from a client computer;

determining that the dynamic data element received from the client computer matches the dynamic data element transmitted to the mobile device; and

initiating the payment transaction by the central server computer comprising the digital wallet with the barcode data after the central server computer determines that the dynamic data element received from the client computer matches the dynamic data element that was sent from the central server computer to the mobile device.

14. The method of claim 13 wherein the two-dimensional barcode encodes a primary account number.

15. The method of claim 14 wherein the primary account number is encrypted.

16. The method of claim 13 wherein the physical payment token is a card.

17. The method of claim 13 further comprising:

transmitting a dynamic verification value to the mobile device after receiving the barcode data.

18. The method of claim 13 wherein the dynamic data element is a dCVV, a one-time account number or a one-time password.

19. A server computer comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, for executing a method comprising

sending an authentication communication from a digital wallet in the server computer to a mobile device, wherein the authentication communication is sent in response to the payment transaction being initiated by a user on a client computer,

receiving barcode data from the mobile device, wherein an image of a two-dimensional barcode on a physical payment token is captured with a camera in the mobile device, and wherein the barcode data is based on the captured image,

generating a dynamic data element when the barcode data is authenticated,

transmitting the dynamic data element to the mobile device,

receiving the dynamic data element from a client computer,

determining that the dynamic data element received from the client computer matches the dynamic data element transmitted to the mobile device, and

initiating a payment transaction with the barcode data after the central server computer determines that the dynamic data element received from the client computer matches the dynamic data element that was sent from the central server computer to the mobile device.

20. The server computer of claim **19** wherein the two-dimensional barcode encodes a primary account number.

21. The server computer of claim **20** wherein the primary account number is encrypted.

22. The server computer of claim **20** wherein the barcode data comprises image data of the two-dimensional barcode.

23. The server computer of claim **19** wherein the physical payment token is a payment card.

24. A system comprising:

the server computer of claim **19**;

the client computer; and

the mobile device, wherein the mobile device and the client computer are configured to communicate with the server computer.

* * * * *